PPTAgent: Arbitrary Code Execution via Python eval() of LLM-Generated Code with Builtins in Scope

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-42079
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 17:16:24 UTC
Updated	2026-05-05 20:19:04 UTC
Description	PPTAgent is an agentic framework for reflective PowerPoint generation. Prior to commit 418491a, PPTAgent is vulnerable

Risk And Classification

Primary CVSS: v3.1 8.6 HIGH from security-advisories@github.com

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

EPSS: 0.000230000 probability, percentile 0.064590000 (date 2026-05-05)

Problem Types: CWE-95 | CWE-95 CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	8.6	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
3.1	CNA	DECLARED	8.6	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Icip-cas	PPTAgent	affected < 418491a9a1c02d9d93194b5973bb58df35cf9d00	Not specified

References

Reference	Source	Link
github.com/icip-cas/PPTAgent/security/advisories/GHSA-89g2-xw5c-v95p	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.con
github.com/icip-cas/PPTAgent/commit/418491a9a1c02d9d93194b5973bb58df35cf...	security-advisories@github.com	github.con
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.